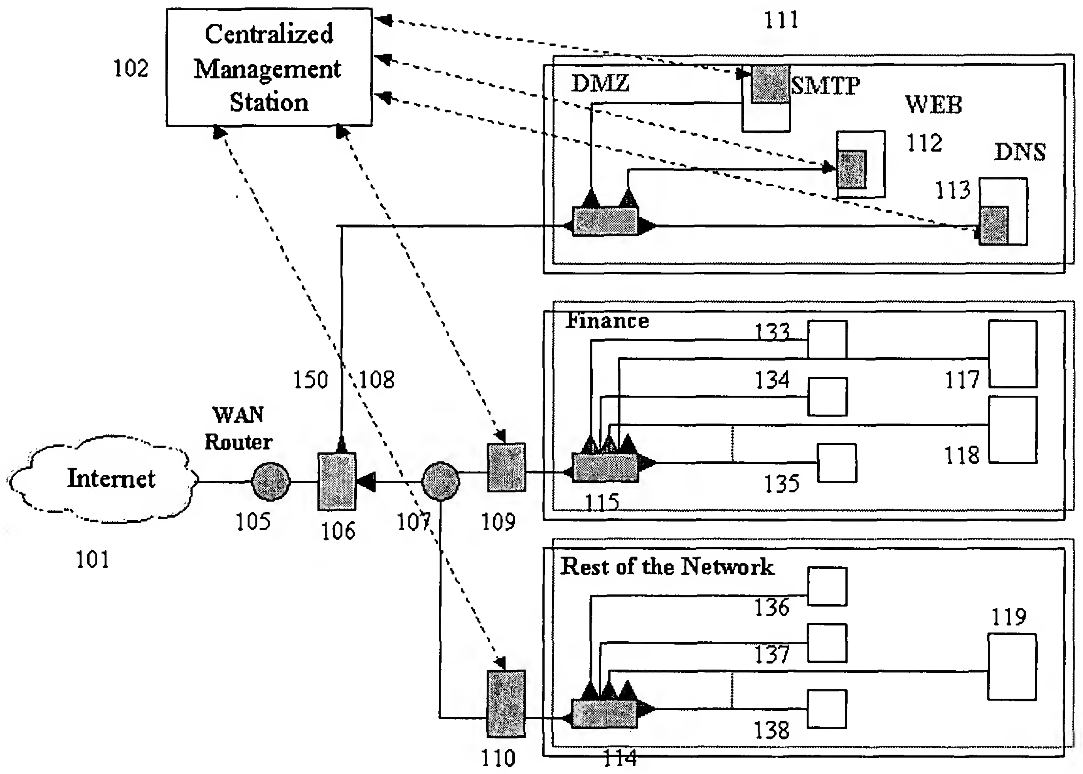


Fig.1: Placement for the Invention Apparatus in an Organization to stop intrusions

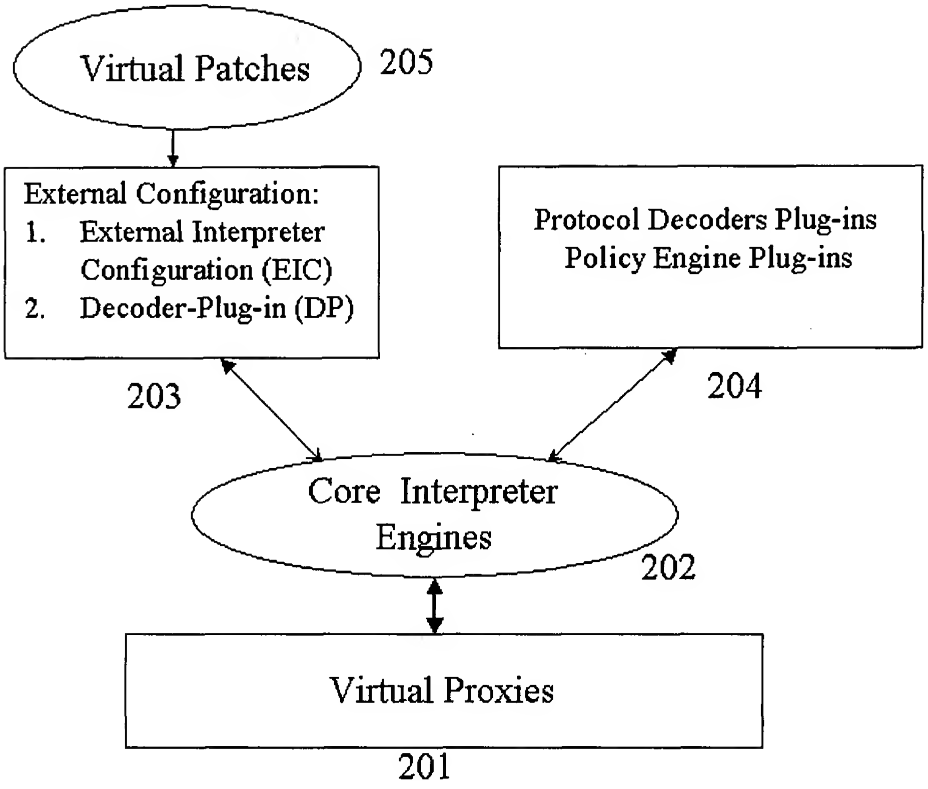


Fig.2: Primary elements of the apparatus and method for stopping intrusion

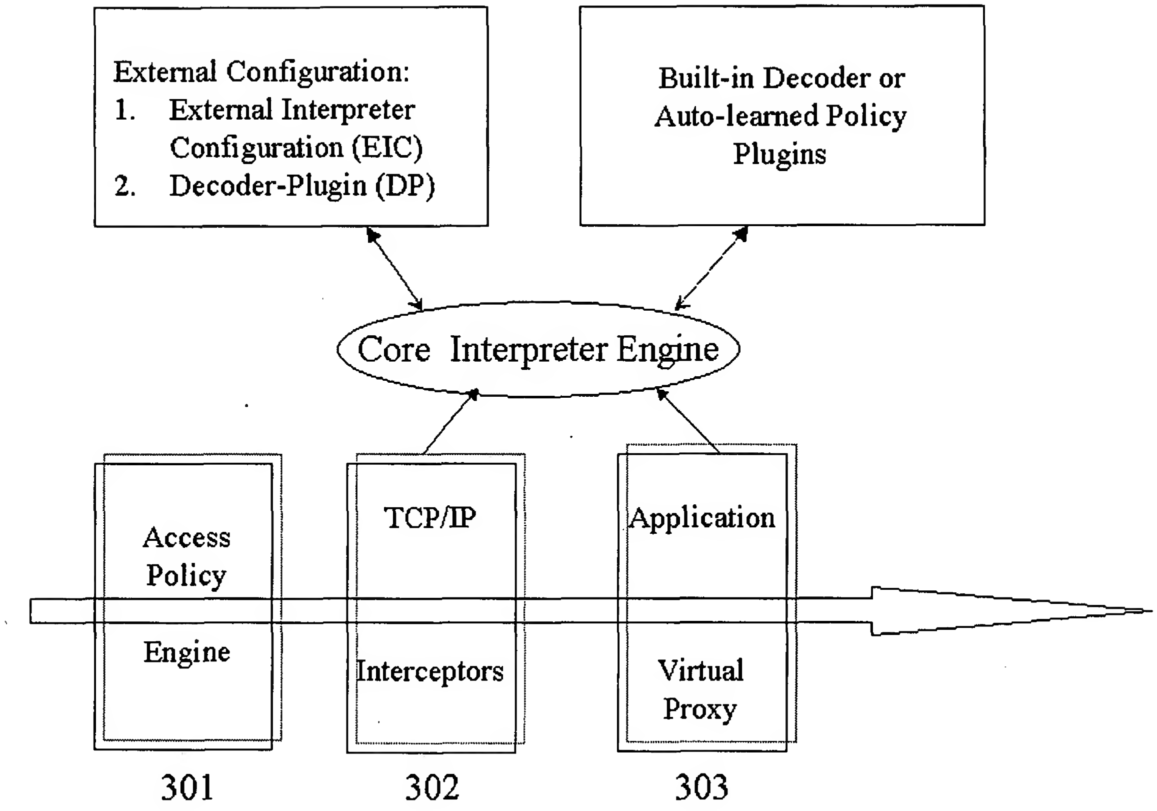


Fig.3: Primary elements of a network based apparatus that uses this invention

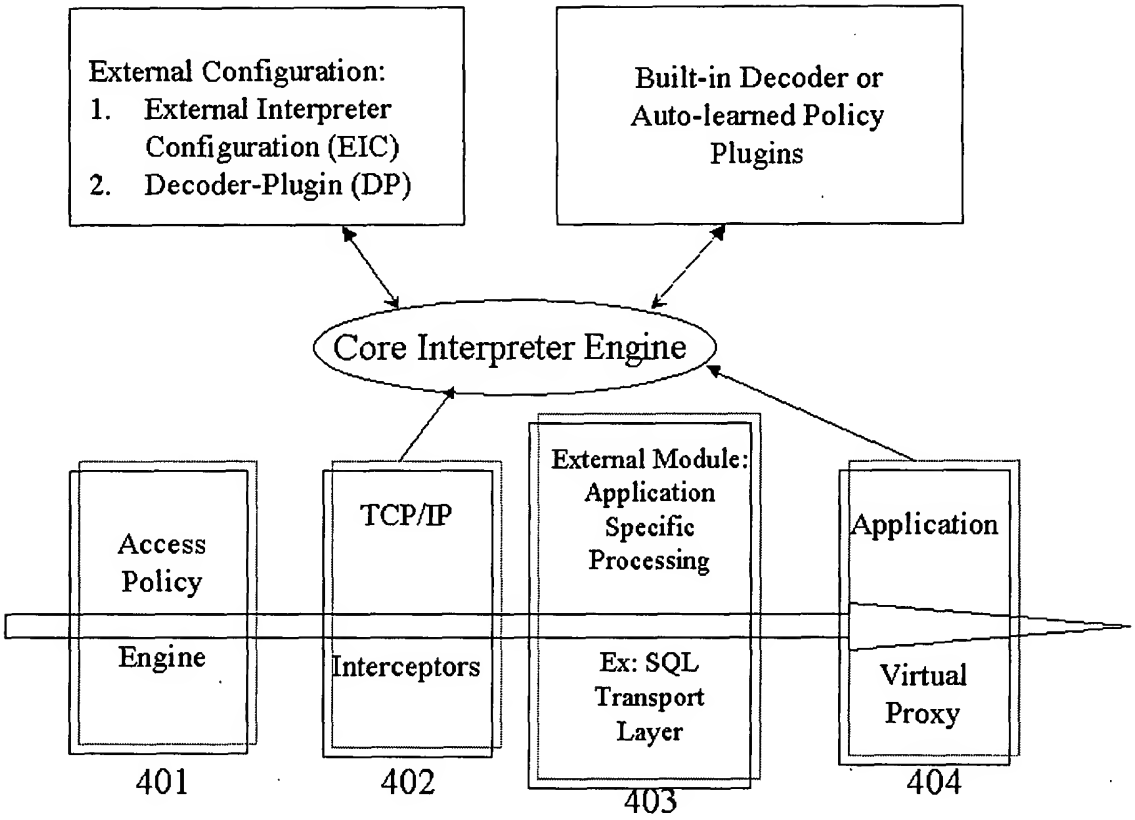
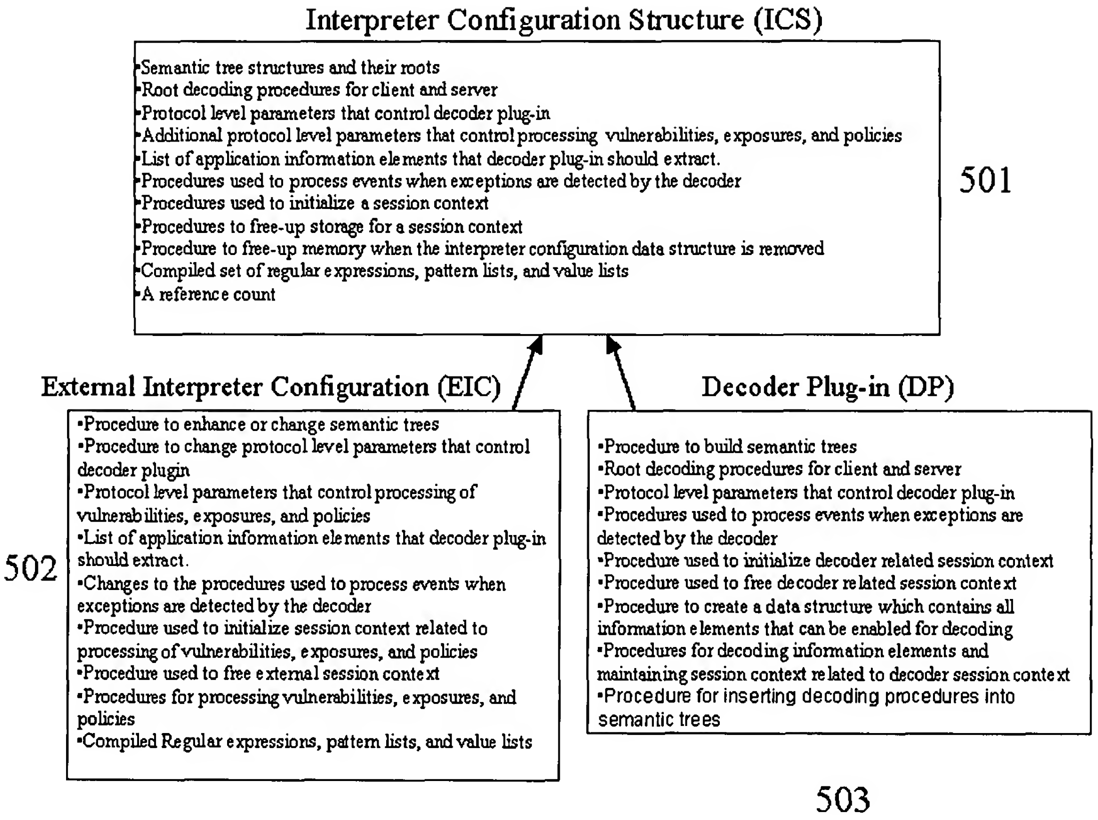

External Configuration:
1. External Interpreter Configuration (EIC)
2. Decoder-Plugin (DP)
Built-in Decoder or Auto-learned Policy Plugins
Core Interpreter Engine
Access Policy Engine
TCP/IP Interceptors
External Module: Application Specific Processing
Ex: SQL Transport Layer
Application Virtual Proxy
401
402
403
404

Fig.4: Primary elements of a host based apparatus that uses this invention



Interpreter Configuration Structure (ICS)

- Semantic tree structures and their roots
- Root decoding procedures for client and server
- Protocol level parameters that control decoder plug-in
- Additional protocol level parameters that control processing vulnerabilities, exposures, and policies
- List of application information elements that decoder plug-in should extract.
- Procedures used to process events when exceptions are detected by the decoder
- Procedures used to initialize a session context
- Procedures to free-up storage for a session context
- Procedure to free-up memory when the interpreter configuration data structure is removed
- Compiled set of regular expressions, pattern lists, and value lists
- A reference count

External Interpreter Configuration (EIC)

- Procedure to enhance or change semantic trees
- Procedure to change protocol level parameters that control decoder plugin
- Protocol level parameters that control processing of vulnerabilities, exposures, and policies
- List of application information elements that decoder plug-in should extract.
- Changes to the procedures used to process events when exceptions are detected by the decoder
- Procedure used to initialize session context related to processing of vulnerabilities, exposures, and policies
- Procedure used to free external session context
- Procedures for processing vulnerabilities, exposures, and policies
- Compiled Regular expressions, pattern lists, and value lists

Decoder Plug-in (DP)

- Procedure to build semantic trees
- Root decoding procedures for client and server
- Protocol level parameters that control decoder plug-in
- Procedures used to process events when exceptions are detected by the decoder
- Procedure used to initialize decoder related session context
- Procedure used to free decoder related session context
- Procedure to create a data structure which contains all information elements that can be enabled for decoding
- Procedures for decoding information elements and maintaining session context related to decoder session context
- Procedure for inserting decoding procedures into semantic trees

Fig.5: Using EIC and DP to build ICS

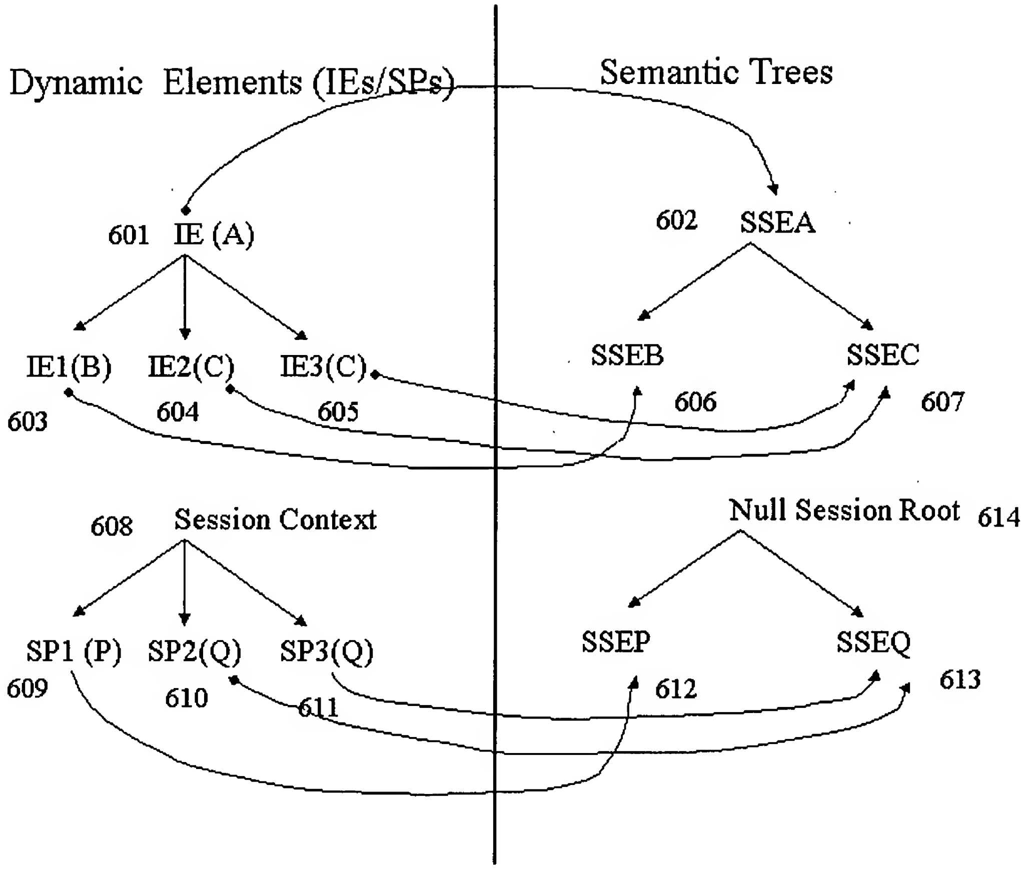


Fig. 6: Relationship between dynamic application elements and semantic trees

	2002	2001	2000
CVE Count	1307	1506	990

Figure 7: Total CVE count on yearly basis

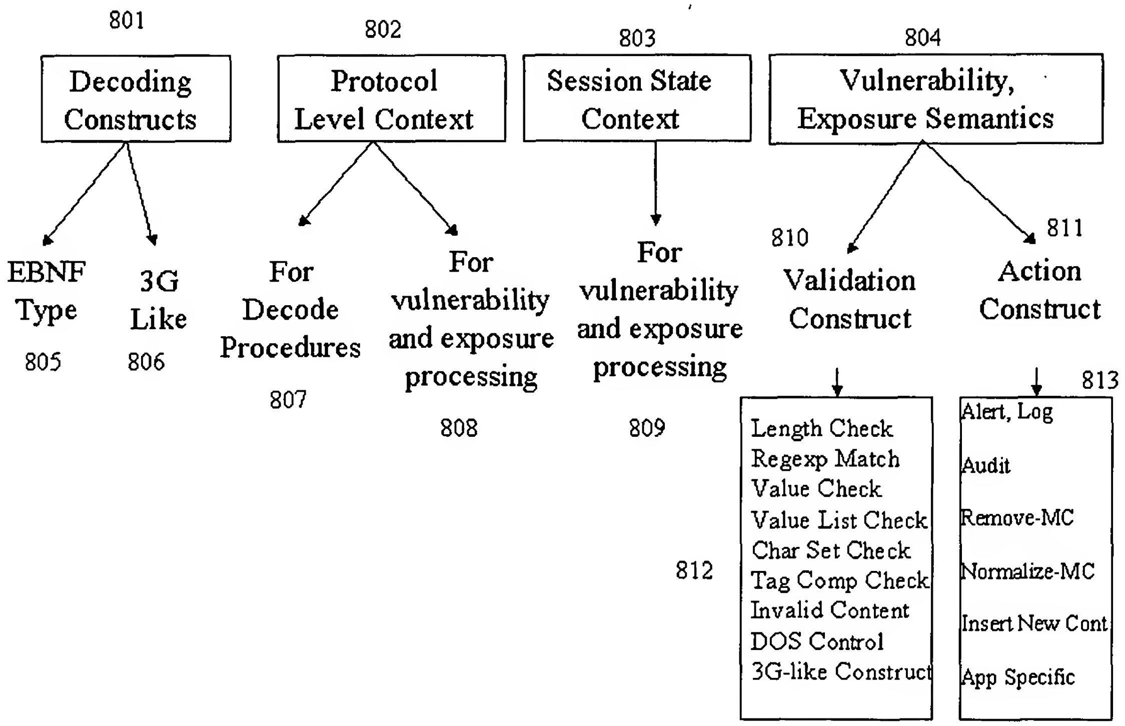


Figure 8: Elements of a method and apparatus for capturing vulnerabilities/exposures.